Uber reveló el lunes más detalles relacionados con el incidente de seguridad que ocurrió la semana pasada, atribuyendo el ataque cibernético a un grupo de hackers que se cree, está afiliado al notorio grupo de hacking LAPSUS$.

> *«Este grupo generalmente usat técnicas similares para atacar a las empresas de tecnología, y solo en 2022 ha violado a Microsoft, Cisco, Samsung, NVIDIA y Okta, entre otros»*, dijo la compañía.

El grupo de hackers con motivación financiera recibió un duro golpe en marzo de 2022 cuando la policía de la ciudad de Londres arrestó a siete presuntos miembros de la banda LAPSUS$ de entre 16 y 21 años de edad. Semanas después, dos de ellos fueron acusados por sus acciones.

El hacker detrás de la violación de Uber, un adolescente de 18 años que se hace llamar Tea Pot, también se atribuyó la responsabilidad de irrumpir en el fabricante de videojuegos Rockstar Games durante el fin de semana.

Uber dijo que está trabajando con *«varias firmas forenses digitales líderes»* mientras sigue la investigación de la compañía sobre el incidente, además de coordinar con la Oficina Federal de Investigaciones (FBI) de Estados Unidos y el Departamento de Justicia sobre lo ocurrido.

En cuanto a cómo se desarrolló el ataque, la compañía de viajes compartidos dijo que *«un contratista de EXT»* vio comprometido su dispositivo personal con malware y sus credenciales de cuenta corporativa fueron robadas y vendidas en la web oscura, lo que corrobora un informe anterior de Group-IB.

La empresa con sede en SIngapur, la semana pasada, dijo que al menos dos de los empleados de Uber ubicados en Brasil e Indonesia estaban infectados con los ladrones de información Raccoon y Vidar.

> *«El atacante intentó repetidamente iniciar sesión en la cuenta de Uber del contratista. Cada vez, el contratista recibió una solicitud de aprobación de inicio de sesión de dos factores, que inicialmente bloqueó el acceso. Eventualmente, sin embargo, el contratista aceptó una y el atacante inició sesión con éxito»,* dijo la compañía.

Al establecerse, se dice que el atacante accedió a las cuentas de otros empleados, lo que equipó a la parte malintencionada con permisos elevados para *«varios sistemas internos»,* como Google, Workspace y Slack.

La compañía dijo además de que tomó una serie de medidas como parte de sus medidas de respuesta a incidentes, incluyendo la desactivación de las herramientas afectadas, la rotación de claves de los servicios, el bloqueo de la base de código y también el bloqueo de las cuentas de los empleados comprometidos para que no accedan a los sistemas de Uber o, alternativamente, la emisión de un restablecimiento de contraseñas para las cuentas.

Uber no reveló cuántas cuentas de empleados se vieron potencialmente comprometidas, pero reiteró que no se realizaron cambios de código no autorizados y que no había evidencia de que el hacker tuviera acceso a los sistemas de producción que respaldan sus aplicaciones orientadas al cliente.

De este modo, se dice que el presunto hacker adolescente descargó una cantidad no especificada de mensajes internos de Slack e información de una herramienta interna utilizada por su equipo de finanzas para administrar ciertas facturas.

Uber también confirmó que el atacante accedió a los informes de error de HackerOne, pero dijo que *«cualquier informe de error al que el atacante pudo acceder ha sido remediado».*

> *«Solo hay una solución para hacer que la [autenticación de múltiples factores] basada en push sea más resistente y es capacitar a sus empleados, que usan MFA basado en push, sobre los tipos comunes de ataques en su contra, cómo detectar*

> *esos ataques y cómo mitigarlos e informarlos si ocurren»,* dijo Roger Grimes, evangelista de defensa basada en datos de KnowBe4.

Chris Clements, vicepresidente de arquitectura de soluciones en Cerberus Sentinel, dijo que es crucial que las organizaciones se den cuenta de que MFA no es una solución milagrosa y que no todos los factores son iguales.

Aunque ha habido un cambio en la autenticación basada en SMS a un enfoque basado en aplicaciones para mitigar los riesgos asociados con los ataques de intercambio de SIM, el ataque contra Uber y Cisco destaca que los controles de seguridad que alguna vez se consideran infalibles están siendo eludidos por otros medios.

El hecho de que los atacantes apuesten por rutas de ataque como los kits de herramientas de proxy adversary-in-the-middle (AiTM) y la fatiga MFA (también conocida como bombardeo rápido) para engañar a un empleado desprevenido para que entregue inadvertidamente códigos MFA o autorice una solución de acceso señala la necesidad de adoptar métodos resistentes al phishing.

> *«Para evitar ataques similares, las organizaciones deben pasar a versiones más seguras de la aprobación de MFA, como la coincidencia de números, que minimizan el riesgo de que un usuario apruebe ciegamente un mensaje de verificación de autenticación»,* dijo Clements.

> *«La realidad es que si un atacante solo necesita comprometer a un solo usuario para causar un daño significativo, tarde o temprano tendrá un daño significativo. Los mecanismos de autenticación sólidos deberían ser uno de los muchos controles defensivos en profundidad para evitar el compromiso»*, agregó Clements.